

“Express Mail” mailing label number:

EV 335894758 US

## **HOST INTRUSION DETECTION AND ISOLATION**

James M. Doherty  
Thomas Lee Adams  
Stephen Mark Mueller

### **BACKGROUND OF THE INVENTION**

#### **Field of the Disclosure**

[1001] The present disclosure relates to methods and systems for intrusion detection.

#### **Description of the Related Art**

[1002] Intrusion detection and other forms of computer system security can be categorized as being either an external scheme or an internal scheme. Examples of external security elements include firewalls and routers. An example of an act performed by an external security element is port monitoring, which comprises watching traffic at critical incoming ports. External security elements may be used to provide protection against denial of service (DOS) attacks. Firewalls can also provide port forwarding and DMZ-type applications. External security elements often do not limit outgoing port connections.

[1003] Internal protection schemes are designed to prevent security breaches by use of file permission, directory access and execution permission. The aforementioned examples of internal protection are usually set as part of a computer's file system. Internal protection schemes prevent unauthorized users from accessing certain aspects of the system that could cause damage or provide unauthorized access to sensitive material.

## **BRIEF DESCRIPTION OF THE DRAWINGS**

[1004] The present invention is pointed out with particularity in the appended claims. However, other features are described in the following detailed description in conjunction with the accompanying drawing in which:

[1005] FIG. 1 is a schematic, block diagram of an embodiment of an intrusion detection system;

[1006] FIG. 2 is a flow chart of an embodiment of an intrusion detection method; and

[1007] FIG. 3 is an embodiment of a configuration file for use in intrusion detection.

## **DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS**

[1008] Disclosed embodiments make use of several computer functions to provide comprehensive intrusion detection and appropriate isolation procedures. The procedures are implemented programmatically and executed in a real-time, continuous manner.

[1009] Particular embodiments are described with reference to FIG. 1, which is a schematic, block diagram of an embodiment of an intrusion detection system, and FIG. 2, which is a flow chart of an embodiment of an intrusion detection method. The system and method provide intrusion detection for a host system 10. The host system 10 comprises one or more computers that are accessible via a computer network 12. Examples of the host system 10 include, but are not limited to, a server computer, a corporate mainframe computer, and a desktop computer. Examples of the computer network 12 include, but are not limited to, an Internet, an intranet, an extranet, a local area network and a wide area network.

[1010] The host system 10 comprises a plurality of network interfaces 14 for interfacing with the computer network 12. For purposes of illustration and example, the host system 10 is depicted to have two network interfaces 14, although those having ordinary skill will recognize that the host system 10 may have an arbitrary number of network interfaces

in practice. Examples of the network interfaces 14 include, but are not limited to, Ethernet interfaces.

[1011] As indicated by block 20, an intrusion detection system daemon 22 of the host system 10 is executed. The system daemon 22 may be started through a normal startup procedure of the host system 10. In embodiments where the host system 10 is UNIX-based, the system daemon 22 may comprise a JTRIP daemon as depicted in FIG. 1.

[1012] As indicated by block 24, the system daemon 22 reads a configuration file 26. The configuration file 26 may be named JTRIP.CONF as depicted in FIG. 1. The configuration file 26 indicates which directories and files in a file system 30 of the host system 10 are to be monitored by the system daemon 22.

[1013] The configuration file 26 comprises a script of a plurality of directives. The directives include a first directive type, “DIR”, that indicates a directory whose members (e.g., all of the files in the directory) are to be monitored by the system daemon 22. A second directive type, “FILE”, indicates a particular file that is to be monitored by the system daemon 22. A third directive type, “CONF”, indicates a configuration file that is to be monitored by the system daemon 22. The system daemon 22 monitors the configuration file identified by “CONF” on a different schedule than vendor-supplied control files identified by “DIR” and “FILE”.

[1014] FIG. 3 shows an example of the configuration file 26. The configuration file 26 comprises four “DIR” directives 32 to tell the system daemon 22 to monitor all members of the `/bin` directory, the `/sbin` directory, the `/usr/sbin` directory, and the `/usr/local/sbin` directory for intrusion. A “FILE” directive 34 tells the system daemon 22 to monitor a file at `/etc/hosts.equiv` for intrusion. A “CONF” directive 36 tells the system daemon 22 to monitor a configuration file at `/etc/pam.conf` for intrusion, but at a different schedule than the other files and directories.

[1015] As indicated by block 40, the system daemon 22 determines which directories, system files and configuration files are to be monitored based on the configuration file 26.

[1016] As indicated by block 42, the system daemon 22 reads a valid known Message Digest 5 (MD5) signature and a correct permission for each file that is to be monitored. The aforementioned information is read from an MD5 database 44 located on a system isolated physically and programmatically from the host system 10. The MD5 signature comprises a 128-bit message digest for each file regardless of the length of the file. The MD5 signature for each file to be monitored is computed in advance and stored in the MD5 database 44.

[1017] As indicated by block 46, the system daemon 22 determines if an intrusion event has occurred. This act is performed repeatedly, for example multiple times (e.g., two or three times) per day.

[1018] The system daemon 22 detects an intrusion when a modification is made to any monitored file or directory in the file system 30, or when an incorrect permission is associated with any monitored file or directory in the file system 30, or when any monitored file or directory in the file system 30 has an improper ownership, or when any monitored file or directory in the file system 30 no longer exists. A modification to a monitored file is detected by computing a current MD5 signature of the monitored file in the file system 30, and comparing the current MD5 signature to the stored, trusted MD5 signature in the MD5 database 44. An intrusion event is detected if the two MD5 signatures differ.

[1019] If no intrusion event is detected, the host system 10 continues in its normal operating mode to allow external access thereto via the network interfaces 14. Typically, the normal operating mode is a multi-user state wherein multiple users can access the host system 10 via the computer network 12.

[1020] If an intrusion event is detected, the system daemon 22 generates an alarm. In response thereto, the host system 10 performs acts to protect the rest of the computer network 12 from a potentially-compromised system. As indicated by block 50, a log is written to a SYSLOGD database 52 that is not located on the host computer system 10 or the MD5 database system 44. The log indicates specifics of the intrusion event, such as a

time, a date, which one or more files and/or directories triggered the intrusion event, a current MD5 signature associated with a modified file, and a cause of the intrusion event. The cause of the intrusion event may indicate a file or directory has been changed, a file or directory no longer exists, an incorrect permission, or an improper ownership.

[1021] As indicated by block 54, one or more commands are issued to the network interfaces 14 to isolate the host system 10 from the computer network 12. In one embodiment, the one or more commands may comprise one or more IFCONFIG down commands.

[1022] As indicated by block 56, one or more commands are issued to take the host system 10 down to a single user state. In one embodiment, the one or more commands comprise one or more INIT 1 commands issued by the operating system of the host system 10. As a result, access to the host system 10 is limited to physical access at the host system 10 itself, e.g., using a keyboard, pointing device, or other user-input device of the host system 10.

[1023] It is noted that the acts indicated by blocks 50, 54 and 56 can be performed either in a different order than depicted in FIG. 2, or in parallel, in alternative embodiments.

[1024] All communications of the system daemon 22 with the MD5 database 44 and the SYSLOGD database 52 are made via port forwarding using Secure Shell (SSH) tunneling or an alternative protocol to securely access a remote computer. This protects the communications from eavesdropping and man-in-the-middle attacks.

[1025] Those having ordinary skill will recognize that the herein-disclosed computer-implemented acts can be directed by computer-readable program code stored by a computer-readable medium. Examples of the computer-readable medium include, but are not limited to, a magnetic medium such as a hard disk or a floppy disk, an optical medium such as an optical disk (e.g., a CD or a DVD), or an electronic medium such as an electronic memory (e.g., a computer's internal memory or a removable memory such as a memory card).

[1026] It will be apparent to those skilled in the art that the disclosed embodiments may be modified in numerous ways and may assume many embodiments other than the particular forms specifically set out and described herein. For example, other data verification methods that map a file of arbitrary length to a fixed-length signature can be used in place of MD5. More generally, alternative data verification methods can be substituted for MD5.

[1027] The above disclosed subject matter is to be considered illustrative, and not restrictive, and the appended claims are intended to cover all such modifications, enhancements, and other embodiments which fall within the true spirit and scope of the present invention. Thus, to the maximum extent allowed by law, the scope of the present invention is to be determined by the broadest permissible interpretation of the following claims and their equivalents, and shall not be restricted or limited by the foregoing detailed description.